UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/656,887	09/05/2003	Rauno Javanainen	81757.0037	1526

466 7590 10/18/2006

YOUNG & THOMPSON
745 SOUTH 23RD STREET
2ND FLOOR
ARLINGTON, VA 22202

EXAMINER	
PATEL, NIRAV B	
ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 10/18/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/656,887	JAVANAINEN, RAUNO	
	Examiner	Art Unit	
	Nirav Patel	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 September 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *05 September 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Nirav B. Patel AU2135

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *9/5/03 (2)*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the application filed on 09/05/2003.

2. Claims 1-13 are under examination.

Claim Rejections - 35 USC § 112

3. Claims 2, 3, 9, 11-13 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 2 contains the phrase **"if either the client or the agent..."**, which does not specifically limit the scope of the claim. Specifically, the term "if" introduces many possibilities on the claim limitations and made the scope of the claim vague and indefinite.

Claims 11 and 12 encompass limitations that are similar to those of claim 2 **(i.e. "if there is correspondence...")**. Thus, it is rejected with the same rationale applied against claim 2 above.

Claim 3 recites the limitation **"the roles"** on line 6 of claim 3, lacks proper antecedent basis. The examiner is interpreting this limitation as "roles".

Claims 9 and 13 encompass limitations that are similar to those of claim 3. Thus, it is rejected with the same rationale applied against claim 3 above.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-3, 7-10 are rejected under 35 U.S.C. 102(e) as being anticipated by Odinak et al (US Patent No. 6,690,289).

As per claim 1, Odinak discloses:

A system for providing authentication of data communication over a communication link (104) between a client (100) and an agent (102) in accordance with an ordinarily insecure network communication protocol [col. 2 lines 66-67, 1-3, col. 3 lines 19-20, col. 5 lines 5-12, col. 5 lines 66-67, col. 6 lines 1-5], the protocol comprising a communal string field (i.e. third portion of the message, MAC) for an appliance in the data communication [Fig. 4, col. 3 lines 19-20], characterized in that, a string to be applied once, based on a shared seed between the client and the agent, is adapted to be incorporated into the communal string field to be transmitted between the client and the agent for authentication [col. 6 lines 6-14, col. 8 lines 16-18], wherein the string is

determined by a substantially similar algorithm at both the client and the agent based on the shared seed [col. 6 lines 32-35].

As per claim 2, the rejection of claim 1 is incorporated and Odinak discloses:

a second string adapted to be applied once, based on the shared seed, is determined if either the client or the agent has applied the once applied string once [Fig. 9, col. 8 lines 51-52, Fig. 8].

As per claim 3, the rejection of claim 2 is incorporated and Odinak discloses:

the transmitted once applied string of a transmitting entity [Fig. 8, step 83] and the generated once applied string of a receiving network entity match for each string calculation round, and any other pair of the strings does not match, wherein the client and the agent comprise a transmitting network entity and a receiving network entity depending on an operational mode of the client and the agent in the communication link, wherein roles can be changed [Fig. 9, col. 8 lines 56-58, 66-67, col. 9 lines 10-15, col. 5-8].

As per claim 7, the rejection of claim 2 is incorporated and Odinak discloses:

the algorithm generates a new string to be applied once, which string is based on the seed and on a secure random logic for being difficult to copy a pattern of a plurality of the strings [Fig. 8, 9, col. 6 lines 16-24, col. 8 lines 15-19].

As per claim 8, the rejection of claim 1 is incorporated and Odinak discloses:

the client and the agent remain synchronized in an operation loop of currently generated and once applied string by an acknowledgement message between the client and the agent [col. 5 lines 66-67, col. 6 lines 1-3, col. 7 lines 57-65].

As per claim 9, the rejection of claim 1 is incorporated and Odinak discloses:

the client or the agent sets an operation in accordance with the data communication unauthorized, if the string to be applied once, which is transmitted therebetween, does not correspond with a generated string to be applied once of a receiving network entity, wherein the client and the agent comprise a transmitting network entity and the receiving network entity depending on an operational mode of the client and the agent in the communication link, wherein roles can be changed [Fig. 7, col. 7 lines 14-20, col. 5 lines 5-8].

As per claim 10, it encompasses limitations that are similar to limitations of claim 1. Thus, it is rejected with the same rationale applied against claim 1 above.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Odinak et al (US Patent No. 6,690,289) and Brainard et al (US Patent No. 6,985,583).

As per claim 4, the rejection of claim 1 is incorporated and Odinak teaches the shared seed [col. 6 lines 13-14, col. 9 lines 2-5]. Odinak doesn't expressively mention the shared seed is based on a on a random number generator.

Brainard teaches:

the shared seed is based on a random number generator and is generated at either one of the client or the agent, and communicated to the one, which did not generate the shared seed [Fig. 1, col. 5 lines 46-50, 58-59].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Brainard with Odinak, since one would have been motivated to verify the identity of the entity [Brainard, col. 1 line 13].

6. Claims 5 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Odinak et al (US Patent No. 6,690,289) and Osmond (US Patent No. 6,044,468).

As per claim 5, the rejection of claim 1 is incorporated and Odinak teaches data exchange protocol [62-63]. Odinak doesn't mention Simple Network Management Protocol (SNMP).

Osmond discloses:

the ordinarily insecure network communication protocol comprises Simple Network Management Protocol (SNMP) [col. 2 lines 66-67, col. 3 lines 1-3, col. 5 lines 61-63].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Osmond with Odinak, since one would have been motivated to provide the security for entities communicating over a data network [Osmond, col. 1 lines 9-10].

As per claim 6, the rejection of claim 1 is incorporated and Osmond discloses:

the communication link (104) comprises Internet [col. 1 lines 18-20, col. 5 lines 61-63].

7. Claims 11, 12 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Odinak et al (US Patent No. 6,690,289) and Graveman (US Patent No. 6,851,052).

As per claim 11, Odinak discloses:

generating a string to be applied once based on the shared seed at both the transmitting network entity and the receiving network entity [Fig. 8, 9, col. 8 lines 23-29, 50-52, col. 9 lines 3-5], incorporating, at a transmitting network entity, the string into the communal string field for transmitting a message in accordance with the ordinarily

insecure network communication protocol [Fig. 4, 8], receiving the message at the receiving network entity [Fig. 7 step 70], checking the string of the communal string field of the message for correspondence with the string, which is calculated, at the receiving network entity, and authenticating the message if there is a correspondence between the string of the communal string field of the message and the generated string [Fig. 7, col. 7 lines 14-20].

Odinak teaches a seed, which is used in common by the sending device and receiving device [col. 9 lines 3-5 i.e. sharing the seed]. The seed is utilized to generate the MAC (i.e. a string) [Fig. 8, 9].

Graveman teaches:

establishing a seed (i.e. initial value I) at the either network entity for sharing the seed with the one network entity, which did not establish the seed, sharing the seed with the one network entity, which did not establish the seed [Fig. 3, col. 5 lines 20-23, 31-32, 44-46].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Graveman with Odinak, since one would have been motivated to verify the integrity of the message [Graveman, col. 1 lines 29-31].

As per claim 12, the rejection of claim 11 is incorporated and Odinak discloses:

generating a second string to be applied once based on the shared seed at both the transmitting network entity and the receiving network entity (i.e. generating the MAC based on new key, col. 8 lines 23-25, col. 9 lines 5-13, Fig. 8, 9], incorporating, at the

transmitting network entity, the second string into the communal string field for transmitting a second message in accordance with the ordinarily insecure network communication protocol [Fig. 4, 8], receiving the second message at the receiving network entity [Fig. 4, 8], checking the second string of the communal string field of the second message for correspondence with the second string, which is calculated, at the receiving network entity, and authenticating the second message if there is a correspondence between the second string of the communal string field of the second message and the generated second string [Fig. 9, col. 9 lines 14-15].

As per claim 13, the rejection of claim 11 is incorporated and Odinak discloses:

the transmitting network entity and the receiving network entity comprise a client and an agent depending on an operational mode of the transmitting network entity and the receiving network entity in the communication link, wherein roles can be changed [col. 5 lines 5-8].

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Field et al (US 6047072) – Method for secure key distribution over a nonsecure communications network.

Jablon (US 2002/0129247) – Cryptographic methods for remote authentication

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nirav Patel whose telephone number is 571-272-5936. The examiner can normally be reached on 8 am - 4:30 pm (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Thanhnga B. Do
AU2135

NBP

10/13/06